X. Following the FCC's Repeal of Title 2 and launch of the AR/XR program revolving around the Plaintiff, Plaintiff King has suffered infractions from multiple outlets who have used those services, including violations and injuries occuring from her residential area County of Lake's Govermental Offices.

89. The Plaintiff has discovered that in her local area, tax funded, Govermental agencies had begun to use the AR/XR "program" revolving around her, including for the use of AR/XR Correctional Outreach Programs, which has put her to suffer through many infractions and injuries by both employees and those that they promote to. The Plaintiff has also filed a Complaint to that County, which may be referenced by the Case No CV-424396 filed at Lake County Superior Court, along with the five restraining orders by case numbers FL-217965, CV-423602, CV-423882, CV-423945 and CV-424321. which include details, backgrounds and proofs of the military base operation that started it. These are also available to read at the following links:

- Case of Lake County: https://docs.google.com/document/d/1SR6_H84ZrZ-e6m25ihI5RQjsYkCfvtDr/edit?usp=drivesdk&ouid=111032409835497544650&rtpof=true&sd=true
- Individual Person Restraining Order and Small Claims Cases: https://drive.google.com/drive/folders/1JFbDLJh8kHT-_5ZhqIIlaxe6Lr1kBcjQ
- General Case Information from all of the above Restraint Order and Small Claims Cases: https://drive.google.com/file/d/1N2uTYo99oB_io_1TvsTm260-cSYuHg2S/view?usp=drivesdk

XI. Online software and media Companies such as Inter Active Corp and Match Group also employ unfair, deceptive and unlawful business practices, including the use AR/XR technology to launch and host several social engineering scams.

90. **Inter Active Corp[100] is Delaware-based software company, which owns Match Group[101] and many other companies.** As it is a Delaware-based company it does not follow many laws imposed by other states and the federal government. It is also much more easier to start businesses in Delaware due to less requirements and restrictions in general. Ultimately, Inter Active Corp and Match Group have not

accomplished. They are a software company that distributes templates alongside their own client and media and services.

91. Following the FCC's removal of the Title II Net Neutrality rules in 2019, Inter Active Corp bought Match Group, which then bought virtually every social-meeting and dating website in the country. This includes websites and apps such as Match, Tinder, Okcupid, Bumble, Hinge, Tinder, eHarmony, Meetme, Badoo, PlentyofFish, Zoosk, EliteSingles and Scout-- all of which the Plaintiff has analysed on multiple occasions after 2020 to find them essentially unsuable due to (I)the almost exclusive amount of fake accounts, and (II)restrictions on which and how many account were viewable.

92. Before Title II was repealed, the Plaintiff and other users of social, meeting, dating and forum websites had the ability to search for users by either key words or area codes, which is a feature that has now been removed from all of these websites and apps. There are also new restrictions on users to only be able to view "persons in their local area", and often pre-selects which and how many of those already-limited accounts a user may view per day. The Plaintiff has collected proof of this which may be referenced at:
https://drive.google.com/drive/folders/1Iw727YgJm3TOFL8AoHr5gIdsGQ09RRZN.

93. As well, the profiles listed on these websites and apps, are all largely fakes. The amount of fake profiles is potentially 100%, and at least closer to that. Many of the profiles, following the pattern of the AR/XR program revolving around the Plaintiff, mimic the image and description likeness of a small amount of certain individuals, repeatedly, all of whom had had some form of contact or introduction to Plaintiff King before. The Plaintiff has signed up accounts in at least 3 different area codes on different apps and websites, and each time, the "local profiles" are fake and mimics, constituting a serious social engineering scam. The Plaintiff has collected proof of this that may be referenced at: https://drive.google.com/drive/folders/1J6P-

94. The Plaintiff's claim that Match Group and other meeting and dating website companies employ gross negligence and several forms of business misconduct often relating to illegal data collection, use and sale/distribution, false impersonation and social engineering are backed up in evidence from multiple sources in the following paragraphs:

95. **Loss due to Social Engineering scams increased rapidly in the years after the pandemic, which incidentally began shortly after Title II was repealed**: "According to the FBI's 2022 Crime Report, victims of scams lost 10.3 billion that year. That marks a 50% increase from the 2021 data. On the other hand, the Federal Trade Commission's Sentinel Network Data Book 2022 shows that losses to fraud increased by over 40% compared to 2021 numbers. One of the biggest reasons for these massive losses to scams is social engineering."[102]

96. By definition, social engineering is the psychological manipulation of people to get them to perform actions or divulge confidential information. "Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources." [103] **One article describes patterns of social engineering scams: ""Social engineering is an illegal activity that accounts for 98% of cyber-attacks. - Social engineering is characterized by attackers coercing victims into divulging sensitive information by pretending to be a known person or legitimate entity. - Identity theft through phishing attacks is the most common form of social engineering. - Over 70% of data breaches start with phishing or social engineering attacks."** [104]

97. Match.com itself has had extensive involvement with lawsuits claiming

that there are many known fake profiles on their websites. **In Feb. 2022 a Class Action Lawsuit was filed against Match.com over unauthorized photo use:** "The class action lawsuit was filed earlier this month in Manhattan Federal Court, and alleges that the company broke copyright laws and committed common law fraud by allowing fake profiles with photos of people who did not give their consent to be used in profiles. The lawsuit seeks compensatory damages in the amount of $500 million and $1 billion for punitive damages. It claims that there are about "3,000 allegedly fake profiles that they say use photos of people who have not consented to their use on the website, including photos of famous actors, military personnel and Facebook users."[105] **Similarly, in Nov 2013, Match was sued 1.5 Billion in the past for unauthirused photo use before:** "A Florida woman has filed a $1.5 billion class-action lawsuit against online dating site Match.com, alleging the website allowed photos of her and thousands of others to be used illegally to create phony profiles intended to dupe romantic hopefuls out of money. The suit also says that Match.com, owned by media mogul Barry Diller's IAC/InterActiveCorp, was aware of the fake profiles as the company approves, edits and posts each profile."[106] **Both of these claims back the general description of the Plaintiff's Complaint against Match Group.**

98. **More evidence of Match's fake profiles scams: In September. 2019: "Match.com and US regulators clash over fake accounts.** The agency claims Match Group misrepresented its internal processes. The owner of dating app Match.com is being sued by US regulators for allegedly tricking people into subscribing to its service. Federal Trade Commission documents detail what it called "deception" and "unfair practices". **It claims Match.com used faked responses to dating profiles to tempt people into paying."[107]** The FTC complaint accuses Match Group of knowingly using "deceptive or unfair practices to induce consumers to subscribe to Match.com and to keep them subscribed." The lawsuit details how Match.com users were messaged by fraudulent accounts. The company then allegedly led consumers to believe that the

communicate with real romantic interests using the ventures to encourage the customer to pay for a subscription. The FTC said that hundreds of thousands of people subscribed to Match.com after receiving communications from fake profiles.

99. More articles go into depth about the existence of, and how to tell if a Match.com profile is fake: "Other times, the people hiding behind fraudulent accounts have more sinister intentions for the people they contact. In fact, it's not uncommon at all for fake bot profiles to be on Tinder or fake Facebook accounts to reach out to seemingly vulnerable people. Sometimes, the "person" behind the profile isn't even human at all. Dating profiles are riddled with bots trying to steal your information or trick you into downloading malicious software."The sites list signs to look out for to spot fake profiles as: They Only Have One Photo, Their Photo(s) Seem Too Perfect, They Have Multiple Profiles, They Send You Links, They Have a Suspicious Number of Connections, Their Conversations Are Incoherent; They ask for too much information or money, They are traveling or working overseas.[108]

100. In Feb 2021: Match Gave Scammers, Predators Access to Dating Apps: "Suit Says A Match Group Inc. investor sued current and former board members in Delaware, claiming they failed to keep sexual predators off many of its dating apps—a practice that has allegedly led to assaults—and "knowingly capitalized on fraud" by letting 'fake love interest' emails past scam filters. Match.com had the ability to detect potentially fraudulent users and block their communications, and 'it did, but only for a fee,' the 167-page lawsuit says. 'For nonsubscribers, on the other hand, Match.com used the fraudulent users to entice membership subscriptions."[109]

101. In April 2017: "A class-action lawsuit was filed against OkCupid for allegedly enticing users to pay to connect with "A-List" users who have "liked" their profile when, according to the complaint, the users who pay the monthly fee learn that most, if not all, of the users who "like" them are not viable dating options because they have inactive accounts. (Perkins et al v. Match Group, Inc. d/b/a OkCupid, Case No. 17

102. In Jan 2022, Match Group Inc (MTCH.O) said it would pay Tinder founders $441 million to settle a case in which the dating app's executives claimed the parent company lowballed the app's value to avoid paying billions of dollars. The lawsuit filed in 2018 had stated that IAC/InterActiveCorp (IAC.O) and subsidiary Match deliberately prevented Tinder founders Sean Rad, Justin Mateen and Jonathan Badeen from cashing in stock options they could exercise and sell to IAC.[110-1]

XII. Inter Active Corp, Match Group's Long-Time Parent Company from 2009 Until 2020, has several complaints filed against them for various similar infractions, as well as other information that does not look good. The Plaintiff has strong cause to believe the company IAC is also involved in illigitimate AR/XR stalking of her, including the use, sale and distribution of her sensitive personal information.

103. **Inter Active Corp[110-2] (IAC) is a software and media holding company that owns or recently did own more than 150 other companies, including Match Group[111].** Examples of other companies they own or have recently owned are Homeadvisor, Yahoo, CollegeHumor, and long list of other more simple media, travel, food, home improvement and "ask how to do this" websites.

104. **In the year 2020, just as the pandemic had started, suddenly IAC dropped 3 of its major companies all in that same year. 1.** College Humor, a very "risky" media channel, was owned by IAC since it was first incirporated in 2006, until the year 2020. "Since then, the company has continued to release content on YouTube and it's streaming service, "Dropout"".[112] **2.** Similarly, in Dec 2020, IAC spun off its long-owned Vimeo service.[113] **3.** As well in 2020, IAC also dropped Match after 11 years of prior ownership from 2009 until 2020, shortly after Net Neutrality rules were repealed, Covid-19 state of emergency and the AR/XR program based around the military base schemevrevolving around the Plaintiff began: "Last year, the companies announced a plan that would see IAC's ownership of Match distributed to IAC's shareholders — a plan that is complete as of this morning."[114] **The Plaintiff believes that IAC distributed it's previously long-owned companies and stock holdings to avoid liability during the pandemic trials. All of the companies that were dropped, the Plaintiff is aware, engage**

in the AR/VR program as well as IAC does.

105. Vimeo, one of IAC's recently dropped companies Vimeo agreed to a USD2.25 million settlement in a lawsuit alleging its artificial-intelligence-based video creation and editing platform collected and stored users' biometric data without consent in violation of Illinois' Biometric Information Privacy Act, SC Media reports. [115]

106. More unfair and deceptive business practices are sited in another artivcle by The Wall Street journal, which learned that Google is considering 'severe penalties' against internet giant IAC over allegedly deceptive practices in it's Chrome extensions: "The browser extra reportedly promise features that never materialize, point users towards additional ads, or even trick users into installing them. A Google audit reportedly found that some of IAC's voting ads not only didn't take users to voter info, but installed the Ask.com toolbar and changed the users default home pages. IAC kept running those ads even after Google told the company to stop."[115]

107. Indeed, the company does not have a good record. In 2008, a lawsuit was filed in Los Angeles accusing IAC's CitySearch of Click Fraud: "The allegations are fairly straightforward. Citysearch sells PPC ads as part of a package of services for small business owners. It promises to proactively screen out invalid clicks in its contract/documentation, but the plaintiffs believe Citysearch isn't doing that job well. The plaintiffs claim this failure constitutes breach of contract, negligence and 17200 unfair practices."[116]

108. Another lawsuit filed in 2020 by a Haverford, Pennsylvania law firm, claims HomeAdvisor's business model is defective, deceptive and fraudulent. Bevilacqua and 1,300 contractors nationwide are seeking to join a class-action lawsuit claiming the company distributed bogus leads, blatantly disregarded the lead budgets of contractors and adopted internal procedures that discourage refunds. It even accuses HomeAdvisor's sales representatives of blatantly lying to service professionals."[117] In March 2022, the FTC Charged HomeAdvisor, Inc. with Cheating Businesses, Including

Small Business Seeking Leads for Home Improvement Projects "Since 2014, Angi affiliate has misrepresented the quality, source of leads, and likelihood they would result in actual jobs", the agency alleged.[118] Another lawsuit against HomeAdvisor was filed in San Francisco District Attorney Brooke Jenkins announced that HomeAdvisor, Inc., and its parent corporation will pay $6.82 million in civil penalties for falsely advertising that their employees had clear background checks. The action filed against them in May 2023 Announces a $6.82 Million Settlement and Permanent Injunction in False Advertising Lawsuit: "By misrepresenting the scope of background checks, HomeAdvisor engaged in inherently deceptive advertising," said District Attorney Brooke Jenkins. "Consumers should be able to trust that claims about background checks performed on service professionals, particularly those who go into their homes, are truthful and accurate."[118-1]

109. Yahoo, one of IAC's branch companies, was charged with a major data breach in 2019 spanning from the years 2012-2016. "From 2012 through 2016, several hacks penetrated Yahoo systems and stole billions of records. Cybercriminals are now trying to trick you into filing a Yahoo claim and get a $100 payment because your personal data was in one of the big Yahoo data breaches. They are sending phishing attacks that look like they come from Yahoo and when you click on the links, you wind up on a fake website that looks like it's Yahoo, but will try to steal your personal information. Don't fall for it!"[119] In July 2018, there was a similar charge: "Shareholders claim that public companies have improperly inflated their stock value either by failing to timely disclose data security incidents or latent vulnerabilities that rendered the company's systems susceptible to a cyberattack.a federal court has preliminarily approved Yahoo!'s $80 million settlement based on multiple hacking incidents. As we reported, Yahoo! suffered two cyber-attacks in 2013 and 2014, which compromised the personal information of billions of users. "[120]

110. In June 2017 in response to CalPERS Lawsuit, IAC Abandoned their plan

to issue Non-Voting Stocks.[121] In June 2008: "The Liberty Media Corporation, the entertainment and Internet retailing company controlled by the billionaire John C. Malone, has **sued IAC/InterActiveCorp in a dispute over IAC's plans to split into five companies.** Liberty, which holds a 30 percent stake in IAC, is seeking unspecified damages and a court order blocking the spinoff.... Mr. Diller, the former head of Paramount Pictures, controls the voting rights of all IAC shares that Liberty owns and has said he will exercise those rights in favor of the spinoff."[122] **This information increases the Plaintiff's suspicion and concern over IAC's business practices, including ever more their willingness to go to some lengths to conceal their deceptive and fraudulent business practices within Delaware and the rest of the United States.**

111. After some research, the Plaintiff has also discovered that IAC is sometimes involved in promoting federal programs bringing internet services to low income induviduals[123], which seems related to her case against proponents of the Federal ACP Plans offered by Assurance Wireless.

112. **Both IAC and Match Group, the source of Plaintiff King's case– since the year 2020, had within their apps and websites removed users ability to control both how to search the sites, restricting them to only one location search, or even no search abilities with limited amounts of pre-selected sets of profiles instead-- and since 2020 these profiles have also become fake impersonations of individuals from the AR/XR program revolving around the Plaintiff. Most of the profiles on Match Group, ect's, websites and apps posing as real persons are indeed not real, and often involve verifiable scams that the company does not filter even with knowledge of it.**

---

[100]IAC (Company)- Wikipedia https://en.m.wikipedia.org/wiki/IAC_(company)
[101]Match Group- Wikipedia https://en.m.wikipedia.org/wiki/Match_Group
[102]Annual Report https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
[103]What is Social Engineering https://www.imperva.com/learn/application-security/social-engineering-attack/
[104]What is Social Engineering https://www.proofpoint.com/us/threat-reference/social-engineering
[105]Lawsuit Filed Against March Over Photo Use tps://www.kgglaw.com/class-action-lawsuits/lawsuit-filed-against-match-over-photo-use

[106]Romance website Match.com sued for $1.5 billion over 'unauthorized' photos https://www.reuters.com/article/us-usa-florida-match/romance-website-match-com-sued-for-1-5-billion-over-unauthorized-photos-idUKBRE9A00Y420131125

[107]Match.com and US regulators clash over fake accounts https://www.bbc.com/news/technology-49652187.amp; Match Investors Want Class Status in Fake Dating Profiles Case https://news.bloomberglaw.com/securities-law/match-investors-want-class-status-in-fake-dating-profiles-case

[108]How To Spot a Fake Profile on Online Dating Apps https://www.makeuseof.com/how-to-spot-fake-dating-profile/; https://www.wymoo.com/blog/match-com-scams-fake-profiles/

[109]Match Gave Scammers and Predators Access to Dating Apps https://news.bloomberglaw.com/tech-and-telecom-law/match-gave-scammers-predators-access-to-dating-apps-suit-says;

[110-1]lass Action Okcupid https://truthinadvertising.org/class-action/okcupid

[111-1]Match Group to pay Tinder founders $441 mln to settle lawsuit https://www.reuters.com/business/match-group-pay-over-400-million-settle-tinder-valuation-case-2021-12-01/

[110-2] (Company)- Wikipedia https://en.m.wikipedia.org/wiki/IAC_(company)

[111-2]Match Group- Wikipedia https://en.m.wikipedia.org/wiki/Match_Group

[112]IAC sells CollegeHumor to executive Sam Reich, resulting in 100+ layoffs https://techcrunch.com/2020/01/08/iac-sells-collegehumor/amp/

[113]IAC announces plan to spin off Vimeo https://www.axios.com/2020/12/22/iac-vimeo-spin-off

[114]IAC and Match Group Complete Full Separation https://www.prnewswire.com/news-releases/iac-and-match-group-complete-full-separation-301086627.html; https://techcrunch.com/2020/07/01/match-group-iac-separaton/amp/

[115] Google may ban IAC's Chrome extensions over 'deceptive' practices https://www.engadget.com/google-may-ban-iac-chrome-extensions-194738382.html

[116]CitySearch Sued for Click Fraud https://blog.ericgoldman.org/archives/2008/05/citysearch_sued.html

[117]HUNDREDS OF CONTRACTORS JOIN CLASS-ACTION LAWSUIT ACCUSING HOMEADVISOR OF FRAUD: 6ABC ACTION NEWS INVESTIGATION https://6abc.com/amp/homeadvisor-fraud-lawsuit-6abc-investigates/5928797/

[118]Charges HomeAdvisor, Inc. with Cheating Businesses, Including Small Businesses, Seeking Leads for Home Improvement Projects https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-charges-homeadvisor-inc-cheating-businesses-including-small-businesses-seeking-leads-home; CLASS ACTION LAWSUIT AGAINST HOMEADVISOR, ANGI AND IAC https://chimicles.com/class-action-lawsuit-filed-homeadvisor-iacinteractive/

[118-1]District Attorney Brooke Jenkins Announces a $6.82 Million Settlement and Permanent Injunction in False Advertising Lawsuit https://sfdistrictattorney.org/press-release/district-attorney-brooke-jenkins-announces-a-6-82-million-settlement-and-permanent-injunction-in-false-advertising-lawsuit/

[119]Scam Of The Week: Yahoo Massive Data Breach Settlement Phishing Attacks https://blog.knowbe4.com/scam-of-the-week-yahoo-massive-data-breach-settlement-phishing-attacks?hs_amp=true

[120]or $80 Million, Yahoo! Settles Shareholder Class Action Claiming Stock Price Losses from Data Breaches https://www.pbwt.com/data-security-law-blog/for-80-million-yahoo-settles-shareholder-class-action-claiming-stock-price-losses-from-data-breaches

[121]Inter Active Corp Abandons Non-Voting Stock https://www.calpers.ca.gov/page/newsroom/calpers-news/2017/interactivecorp-abandons-plan-non-voting-stock

[122]Stakeholdwr Sues IAC Over Break Up Plan https://www.nytimes.com/2008/01/26/technology/26liberty.html

[123]Delaware officials are mounting a campaign to tell lower-income families about a federal program that can cut their costs for broadband internet service. https://townsquaredelaware.com/delaware-federal-program-to-lower-internet-costs/

XIII. There are many examples of Homormorphically Encrypted web filtering tools to be highly effective for most purposes.

113. A paper available at https://drive.google.com/file/d/1JCRmdSL9gezGmTNYi4dhwMZJKXD62c8R/view?usp=drivesdk called Should Internet Service Providers be Liable for Cyberstalking on their Websites?[123] details efforts and the landscape based around holding Internet Service Providers liable for 3rd Party Content through their services. The paper describes in depth past cases and the current landscape of cyberstalking and ISP liability. Begin article---

114. "47 USC 230(c) provides immunity from civil liabilities to ISPs (1-2). The ISP immunity provided by 47 USC 230(c) is generally involved in cases involving defamation, libel, and slander causes of action.[124] Moreover, Congress explicitly provides in section 230(e)(1) that this immunity will not necessarily apply in criminal cases. Therefore, while immunity provided by section 230 protects ISPs from civil liability, protection from criminal liability remains unclear. Problems arise when an Internet user takes on someone else's identity, such as a case where Dellapenta posted messages posing as his victim. When testifying before Congress regarding Dellapenta[125], Deputy Attorney General Eric Holder stated: 'Current federal law does not address those situations where a cyberstalker uses unwitting third parties to bombard a victim with messages, transmits personal data about a person-- such as the route a person's children walk to school-- in order to place a person or his family in fear of injury, or send an email or other form of communication under someone else's name with the intent to abuse, harass or threaten that person.' The DOJ report on cyberstalking also discussed this situation:

115. "[A] A cyberstalker can dupe other internet users into harassing or threatening a victim by using internet bulletin boards or chat rooms. For example, a stalker may post a controversial or enticing message on a board under the name, phone

number, email address of the victim resulting in subsequent response being sent to the victim. Each message-- whether sent from the actual cyberstalker or others-- will have the intended effect upon the victim, but the cyberstalker effort is minimal and the lack of direct contact between the cyberstalker and the victim can make it difficult for law enforcement to identify, locate and arrest the offender;

116. "Considering these potential problems, should the ISP require some kind of consent from those participating, in the case the posting is not what it seems? Should the ISP then be liable if it does not get that consent? ... Congress found 'No' in this case, however;

117. "Despite the immunity offered by section 230, there may be another way for ISPs to be held liable for the actions of its subscribers. According to the DOJ report on cyberstalking, 'ISPs almost uniformly have provisions in their online agreements specifically prohibiting abusive or harassive conduct through their services and providing that violations of these terms would result in termination of the account.[126]';

118. "This type of subscriber agreement works in theory, but realistically, ISPs are not actually capable of sifting through the thousands of new web sites that pop up on the internet every day to discover violations. Once a subscriber sets up a website, it can be readily modified at a moments notice;

119. "Since web sites can be modified frequently, ISPs do not have the resources to perpetually monitor the content of a subscriber's website." --- end article.

120. A solution to the above problem would obviously be homormorphic encryption[123], a filtering tool that allows information to be processed internally without viewing or exposing the data to become vulnerable. The filters are also highly customizable, inducing minimal manual intervention, and save time. An example of a good Homormorphically Encrypted web tool is the company TwoHat, which on its webpage advertised the extensive design features of their product.[127] This is one of many examples of a program that uses Homormorphic Encrytion[128] and Grounded

Theory[129] in action.

121. The Plaintiff has done some research on these issues since learning of them, and has written a paper called Privacy Protective Surveillance[130] which overlays the ideas proposed in other papers, one also called Privacy Protective Surveillance[131] and one called Privacy by Design[132], but in more practical and applicable terms. Privacy Protective Surveillance also uses both Homorporic encryption and grounded theory, and like most things that do, she believes that it is an extremely viable, easy and effective method. The Plaintiff has put a lot of effort into researching into multiple categories and sources in order to compile the paper, and believes that it could be of good help as a guidelines for setting Internet regulation infastructure policies.

[123-1]Should ISPs be Liable for Cyberstalking on their Websites? https://drive.google.com/file/d/1JCRmdSL9gezGmTNYi4dhwMZJKXD62c8R/view?usp=drivesdk
[124]Lunney vs Prodigy Services Co., 723 N.E.2d 538, 543 (N.Y. 1999); Zeran Vs Am. Online Inc., 129 F.3d 327 (Fourth Circuit 1997)
[125] dellapenta
[126] ISP policy
[127]Two Hat Web Filtering https://www.twohat.com/: https://www.twohat.com/solutions/content-moderation-platform/
[128]Homomorphic Encryption https://blog.chain.link/homomorphic-encryption/#:~:text=Homomorphic%20encryption%20is%20a%20cryptographic,through%20various%20algorithms%20and%20analyses.
[129]What is Grounded Theory https://delvetool.com/groundedtheory
[130]Plaintiff King's Privacy Protective Surveillance Application Blueprint https://drive.google.com/file/d/1N2uTYo99oB_io_1TvsTm260-cSYuHg2S/view?usp=drivesdk
[131]The Original Privacy Protective Surveillance https://drive.google.com/file/d/1I0NBWJAA6fyRfVQF8wHdqD1p6SFhufLh/view?usp=drivesdk
[132]Founding Principles of Privacy by Design https://www.onetrust.com/blog/principles-of-privacy-by-design/

XIV. Many AR/XR Platform software for Contact Lens, Glasses, Headsets and fNIRS technologies run on Blockchain technology, which is known to be very harmful.[133]

122. A Blockchain is a decentralized public ledger that records "cryptocurrency" or "fake internet money" transactions.[134]

123. **Blockchains and cryptocurrency are widely known to have a bad reputation. There are numerous, widespread, uncountable and extreme violations of many federal and state laws that occur through decentralized currency.[135]**

124. The ar-03397-JD Document 1-1 Filed 06/05/24 Page 24 of 55 are

1 As it is purely peer to peer with no central regulation, many people are frequently scammed without remedy.

2 The Blockchain ledger is immuntable, meaning that transactions recorded are peanent and can't be changed. That means that all transactions, whether good or bad, shown on the ledger. That means if one takes of advantage of the platform to steal from or defraud an individual, there are no remedies, and furthermore the tort remains broadcast on the public ledger. This system needless to say promotes illegal behavior.

125. Again, Nvidia Omiverse and Metaverse are known to operate their platforms on Blockchain systems. Here it is essential to note that AR/XR, in difference from Virtual Reality, uses, real-life, often teal-time data harvesting from the real world, and then transcribed that real-world data onto Virtual areas where there is a huge lack of regulation. **This means that any unknowing individuals data can be harvested, have content transcribed in their likeness to illegal degrees. These are commonly called "deep fakes" or "synthetic reality".[137]**

126. The term “deepfake” comes from two separate words – deep learning and fake – which uses artificial intelligence technology to create fake pictures or videos in the image of an original video or image. The creator can utilize special software programs to create the picture or video by face swapping. **This has become a problem because it can violate the victim’s privacy rights and public image. Many victims of Deepfake technology cite the content for either being obviously explicit and profane, or that these Deepfake are made in their likeness with often certain traits that are altered to make them out of character or spread false information. [138]**

127. Plaintiff King was targeted by extremely high amounts of Deepfake technology spam and scams through the use of Defendants AR/XR Headsets, Glasses and Contact Lens and AR Platforms. Deepfakes can cause various types of torts.[20]

Plaintiff King herself was targeted by many and with obvious non acceptance. There are many articles online about "malicious Deepfakes"[139]. Plaintiff King encountered Deepfakes who generally copied her physical image, including her name and various personal details (like job, house appliances, accessories, or key rings, or are these NFTs?), general topics that she had spoken about, her voice, as well as things that were in her surroundings. Those who use these Deepfakes have tracked her GPS location[140], and seem to have tried to encourage others to do so by giving this information out to unknown users of AR/XR Headsets, Glasses, Contact Lens and AR Platforms on the internet.

---

[134]See How to use Blockchain in the Meta versehttps://www.google.com/url?sa=t&source=web&rct=j&url=https://blockchain.oodles.io/blog/how-to-use-blockchain-in-the-metaverse/&ved=2ahUKEwj3o_fq46r_AhVgFVkFHXDeAHIQFnoECCYQAQ&usg=AOvVaw2rEcWNZU7MSOntzHRKNSLZ; Technology and Legal issues Behind Metaverse www.abovethelaw.com/2022/09/the-technology-and-legal-issues-behind-metaverse/

[135]See What is a Blockchain https://www.forbes.com/advisor/investing/cryptocurrency/what-is-blockchain/;

[136]There's no Good Reason to Trust Blockchain Technology https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/; Emerging Scams and Phishing Risks in the Metaverse https://www.pwc.com/us/en/tech-effect/cybersecurity/emerging-scams-and-phishing-risks-in-the-metaverse.html

[137]See What is a Deepfake https://www.businessinsider.com/guides/tech/what-is-deepfake?amp; https://www.lexisnexis.co.uk/legal/news/what-to-do-about-deepfake-metaverse-libel-threat-to-publishers;

[139]Rise of deepfakes: who can you trust in the metaverse? https://cybernews.com/security/rise-of-deepfakes/

[140]The Time to Stop a Toxic Metaverse is Now https://mediawell.ssrc.org/news-items/the-time-to-prevent-a-toxic-metaverse-is-now-centre-for-international-governance-innovation/;

XVI. Brain Computer Interface Technology is illegally used through AR/XR Headsets, Glasses and Contact Lens and on AR/XR Platforms. [141]

128. fNIRS imaging conducted through satellite or drone video footage can and does record an individual's thoughts and translate them into text and audio transcripts through satelites.[142]

129. Defendants are known to use, promote, and harvest data from these technologies, using illegal satelite footage, without disclosure or agreement of those it takes data from.

130. The fNIRS brain scanning process is currently illegal under all of the statues listed in the Violations and more.

131. The Plaintiff has been a victimized by the use of this technology through the AR/XR devices, programs, platforms and applications on many re-occuring occasions and many of which were both potentially and actually very dangerous to her, as well as deteriorating her health through lack of sleep, being stolen from and assaulted, and being stalked and harassed. She has been uncessararily andunlawfully injured, and demands injunction of the practices and compensation for damages.

132. Citizens are not given notice nor their consent when it takes place, and there are is no legitimate reasons for the use of the privacy-invading technology in many cases.

XVII. Image based Eye tracking Technology is illegally used through AR Glasses and Contact Lens and on AR/XR Platforms[143]

133. fNIRS imaging conducted through satellite or drone video footahe can and does record image-based eye tracking data.[144]

134. Defendants are known to use, promote, and harvest data from these technologies, using illegal satelite video footage, without the disclosure or agreement of those it takes data from.

135. The fNIRS eye scanning process is currently illegal under all of the statues listed in the Violations and more.

136. The Plaintiff has been a victimized by the use of this technology through the AR/XR devices, programs, platforms and applications on many re-occuring occasions and many of which were both potentially and actually very dangerous to her, as well as deteriorating her health through lack of sleep, being stolen from and assaulted, and being stalked and harassed. She has been uncessararily andunlawfully injured, and demands injunction of the practices and compensation for damages.

137. Citizens are not given notice nor their consent when it takes place, and there are is no legitimate reasons for the use of the privacy-invading technology in many

XVIII. AR/XR Headsets, Glasses, Contact Lens and Platforms are capable of invisibly recording and watching video and audio in violation of several laws, which they then might seek to upload to other platforms without authorization, which promotes Deepfakes, fake news and content, fraud, theft and and phishing scams.

138. Meta particularly, and Nvidia, are known to go behind the scenes with their applications and policies. Their prior lawsuits, as noted above, ended with admittance. In the Cambridge Data Breach[145], they agreed to pay $725 million for illegally harvesting data. The Alliance for Creativity sued them for illegally streaming content that they did not own on their Omniverse Channel.[146] In the case against GPRD[147], users were upset about 1- the kinds of data that Meta collected and 2- the ways and means by which the data was collected. The case is still standing. In addition, on the Metaverse app, there is a lot of controversy over copyright and image rights on their platforms, including 3 major cases concerning copyright infringement through their live stream labeling and "deep fakes".[148]

139. Meta and Nvidia, being pioneers of technological development, are known to use many of the most advanced technologies, including high resolution satelite imagery through the company Maxar Technologies explicitly for their AR/XR platforms.[149] High resolution satelite imagery can be used to conduct fNIRS[150], which can produce both image based eye tracking technology and brain computer interfaces[142] which can respectively allow one to see images that an individual's eye sees[143],[144], and amoung other things turn thoughts into text, which can be rendered as well into audio through live stream logs.[142] **This technology application simply requires an uncomplex HD video camera, meaning that eye tracking can be read through a phone camera or webcam, but theseare not the only means that it can be accomplished. Augmented reality is made with live content, and this also encompasses the use of SAR and Optical imaging satelites, which the Metaverse is also confirmed to use.**

[141]Nine insights into the Metaverse from the QI Stage https://today.duke.edu/story/nine-insights-into-the-metaverse-from-the-qi-stage
[142]Ai makes non invasive brain reading possible by turning thoughts into text https://amp.theguardian.com/technology/2023/may/01/ai-makes-non-invasive-mind-reading-possible-by-turning-thoughts-into-text; Functional Near infared Spectroscopy: Enabling Routine Functional Brain Imaging https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5810962
[143]In the Metaverse companies will Track your gaze https://time.com/6188956/metaverse-is-left-unregulated-companies-will-track-gaze-emotions
[144]Funtional Near Infared Spectroscopy and it's Applications https://www.arcgis.com/home/item.html?id=4e681ff69e0e4b90866bb6a2e03db24a
[145]See Meta Faces Lawsuit to stop ' Surveillance Advertising' https://www.theregister.com/AMP/2022/11/23/meta_surveillance_advertising_high_court/&ved=2ahUKEwix8_X366r_AhViJ30KHUzNAHMQFnoECA4QAQ&usg=AOvVaw08nouwHvPe95kWWK9-ZeX6
[146]See Ace wins $50 million Against Omniverse https://www.trademarksandbrandsonline.com/news/ace-wins-50m-damages-and-injunction-against-omniverse-5574
[147]See Meta Faces Lawsuit to stop ' Surveillance Advertising' https://www.theregister.com/AMP/2022/11/23/meta_surveillance_advertising_high_court/&ved=2ahUKEwix8_X366r_AhViJ30KHUzNAHMQFnoECA4QAQ&usg=AOvVaw08nouwHvPe95kWWK9-ZeX6
[147] See Meta Faces Lawsuit to stop ' Surveillance Advertising' https://www.theregister.com/AMP/2022/11/23/meta_surveillance_advertising_high_court/&ved=2ahUKEwix8_X366r_AhViJ30KHUzNAHMQFnoECA4QAQ&usg=AOvVaw08nouwHvPe95kWWK9-
[148]Live Deepfake in the Metaverse https://volucap.com/deepfakes-in-the-metaverse/
[149]The Metaverse needs Satelite imagery https://blog.maxar.com/earth-intelligence/2022/the-real-world-metaverse-needs-satellite-imagery
[150]Funtional Near Infared Spectroscopy and it's Applications https://www.arcgis.com/home/item.html?id=4e681ff69e0e4b90866bb6a2e03db24a

---

XIX. Injury to the Plaintiff from Defendants Federal Trade Commission, Federal Communications Commission, Meta, Nvidia, Maxar Technologies, Google, Securus/Aventiv Technologies, Global Tel-Link/Viapath, Inter Active Corp, Match Group, Bumble, Spark Networks, Meet Group Inc, Newcom Networks, and any other other related Satellite, Internet Platforms/Services/Media Companies, or other persons or entities that use AR/XR devices, programs, platforms and applications that view illegally-taken satellite video, audio and fNIRS footage of the Plaintiff.

140. As an immediate, diect, and proximate result of Defendants Federal Trade Commission, Federal Communications Commission, Meta, Nvidia, Maxar Technologies, Google, Securus/Aventiv Technologies, Global Tel-Link/Viapath, Inter Active Corp, Match Group, Bumble, Spark Networks, Meet Group Inc, Newcom Networks, and any other other related Satellite, Internet Platforms/Services/Media Companies, or other persons or entities that use AR/XR devices, programs, platforms and applications that view illegally-taken satellite video, audio and fNIRS footage of

the Plaintiffs' conduct, Defendants injured Plaintiff King.

141. Plaintiff King had high and unknown degrees and types of their personal information exposed to unknown users of the AR/XR Platforms and Products, and innumerable types of torts inflicted through them, which have caused untollable degrees and types of damages, including physical harm, mental and emotional harm, and fiscal harm.

COUNT I
Violation of 47 U.S.C. 605

142. All of the foregoing paragraphs are re-alleged as if fully set forthherein.

143. This cause of action is brought pursuant to 47 USC 605 pertaining to Unauthorized publication or use of communications. **47 USC 605 prohibits "persons who transmit or receive wire or radio communications" from divulging such communications except to authorized persons.**

144. Accordingly, Defendants' conduct, specifically their lack of compliance to modern regulatory and record keeping standards concerning their use of AR/XR devices, programs, platforms and applications violates 47 USC 605 in that **they are engaged in illegally viewing and recording satelite video footage of places and persons outside of their warranted jurisdiction, including the divulganced of audio and videos that were intercepted through wiretapping places of expected privacy.**

145. Defendants actions led to direct, foreseeable, and proximate injury to Plaintiff King and the other class members.

146. As a consequence of of the Federal Communications Commission, Meta, Nvidia, Maxar Technologies, Google, Securus/Aventiv Technologies, Global Tel-Link/Viapath, Inter Active Corp, Match Group, Bumble, Spark Networks, Meet Group Inc, Newcom Networks, and any other other related Satellite, Internet Platforms/Services/Media Companies, or other persons or entities that use AR/XR devices, programs, platforms and applications that view illegally-taken satellite video, audio and fNIRS footage of the Plaintiff, Plaintiff King suffered injuries and uncertainable loss, insofar as they (I)have had private communications obtained through satelite communications divulged to unauthorized persons, (Ii) have been injured in several forms on many occasions because of how and what kinds of information was divulged.

147. Plaintiff King is entitled to:

a. Injunction from the future illegal data collection and use in violation of 47 USC 605.

b. Actual damages and/or statutory damages;

c. Punitive damages; and

d. Reasonable attorney's fees.

COUNT II
Violation of the 4th Amendment

148. All of the foregoing paragraphs are re-alleged as if fully set forthherein.

149. This cause of action is brought pursuant to the 4th Amendment.

150. The 4th Amendment provides "protection from warrantless searches of places or seizures of persons or objects, in which they have a subjective expectation of privacy that is deemed reasonable".

151. The 4th Amendment defines **"a reasonable expectation of privacy" as: residences, hotel rooms, or public places that have been provided by businesses or the public sector to ensure privacy,** including public restrooms, private portions of jailhouses, or phone booths.

152. **Defendants', in not regulating and recording activities conducted on and through their AR/XR devices, programs, platforms and applications knowingly and intentionally violate many state and federal laws.**

153. **Defendants' actions led to direct, foreseeable and proximate injury to Plaintiff King.**

154. As a consequence of Defendants' deceptive marketing scheme, Plaintiff King havs suffered uncertainable loss, insofar as they (i) were the target of unwarranted surveillance conducted by aerial satelittes which follow a person's movements, as well as the illegal uploading and sharing of that content through AR/XR Headsets, Glasses, and Contact Lens and onto AR Platforms and (ii) were surveilled by the aerial satelites and/or drones within areas of expected privacy, namely their residences, hotel rooms, and all public areas where privacy is as

were expanded and (iii) more sensitive personal data collected and distributed to unknown, unauthorised, and undocumented individuals who used that data to cause harm to her.

155. Plaintiff King is entitled to:

a. Injunction from future illegal data collection and use practices;

b. Actual damages and/or statutory damages;

c. Punitive damages;

d. Reasonable attorney's fees.

COUNT III
Violations of the Electronic Communication Privacy Act

156. All of the foregoing paragraphs are re-alleged as if fully set forthherein.

157. This cause of action is brought pursuant to the Electronic Communications Privacy Act.

1. Title I of the Electronic Communications Privacy Act prohibits the intentional actual or attempted interception, use, disclosure, or **"procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication."**

2. Title II of the ECPA **protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses.**

158. The Degendants are known to allow their programs, applications and devices to use illegally-obtained aerial satelites video or drone imagery to stalk and target victims.

159. Defendants knowingly use and promote the AR/XR programs, applications and devices without properly regulating and recording illegal, unauthorused, abusive or fraudulent activity that is made through the programs, applications and devices, which caused various damaged to the Plaintiff by way of the

160. Plaintiff King has in fact had their data illegally harvested, and in addition to being a victim of "deepfake" technology throughout some AR/XR platforms, has also fallen victim to the revelation of sensitive personal data exposure on these platforms, such as their name, GPS location, address, etc. **Defendants knew or should have known that because of their lack of permissions, adherance to compliancy to data, privacy and civil laws, and the flatly illegal types of data that they did share, that their content would cause harm to the Plaintiff.**

161. Because of Defendants' promotion and use of the AR/XR devices, programs, applications are both unrecordered and unregulated for violations of state and federal laws, the Defendants violate the Electronic Communications Privacy Act.

162. Plaintiff King is entitled to:

a. Injunction from future illegal data collection and use practices in violation of ECPA.

b. Actual damages and/or statutory damages;

c. Punitive damages;and

d. Reasonable attorney's fees.

COUNT IV
Violation of California Penal Code Section 637.7

163. This cause of action is brought pursuant to California's Penal Code 637.7.

164. **The California Penal Code 637.7 prohibits "the use of an electronic tracking device to determine the location or movement of a person".**

165. **The use of several different technologies by Defendants, including SAR and Optical Satelites imaging, fNIRS imaging, and GPS tracking, violate the California Penal Code 637.7.**

166. **Plaintiff King has been a frequent victim of location-based stalking by the Defendants and those whom they, both formally and informally, have illegally**

authorized to use the AR/XR devices, programs, platforms and applications. Through means of unauthorised data collection and use through the formentioned means, the programs, applications and devices have also revealed her name, address, GPS location, and various other sensitive personal information to unknown, individuals.

167. Defendants have violated California's Penal Code Section 637.7 in that their programs, applications and devices neither properly regulate or record whether and what kinds of sensitive information that the programs, applications and devices may collect and use, including by neglecting to follow state and federal stauatory accordances concerning personal addresses and real-time GPS tracking of persons, which might then be divulged to unknown amounts of unknown, unauthorised individuals through those platforms and products

168. The Defendants negligant practices concerning their lack of regulation and record keeping through their AR/XR programs, applications and devices, caused much harm to the Plaintiff. Indeed, the harm to Plaintiff King from this conduct is substantial. Plaintiff King suffered substantial injuries as alleged herein and is due injunction from the company's illegal practices, and damage compensation .

169. Plaintiff King was victimized bcause of the current noncompliant regulation and record keeping methods of the AR/XR devices, programs, platforms and applications, and had no way of reasonably avoiding the injury they suffered.

170. Plaintiff King is entitled to:

a. Injunction from future unwarranted location and movement tracking;

b. Actual damages

c. Punative damages and

d. Reasonable attorneys fees.

COUNT V
Violation of the Copyright Act

171. This cause of action is brought pursuant the Copyright Act.

172. The Copyright Act protects copyright owners' rights to produce, prepare and distribute their works.

173. Copyright infringement occurs when a copyrighted work is reproduced, distributed, performed, publicly displayed, or made into a derivative work without the permission of the copyright owner. Examples of copyright material are: (1)literary works; (2)musical works, including any accompanying words; (3)dramatic works, including any accompanying music; (4)pantomimes and choreographic works; (5)pictorial, graphic, and sculptural works; (6)motion pictures and other audiovisual works; (7)sound recordings; and (8)architectural works.

174. Defendants are confirmed to not properly regulate or record whether their AR/XR programs, applications and devices engage in viewing illegally-obtained, aerial Satelite video feeds that use SAR and Optical imaging. As previously noted, privately owned SAR and Optical Satelites are currently allowed to make images of up to 35 centimeters of resolution, which can see things as small as a mailbox, and can cut through cloud cover, as well as see through walls. Satelites are now also equipped with advanced target-tracking technology, meaning that they can to a degree follow a designated moving targets with AI applications. It is obvious that the resolution to which videos and taken from these presumably privately-owned satelites are of higher resolution than what is allowed, as the pictures taken from the satelites can seem to detect many small details. This is an illegal satelite video stream.

175. The above mentioned satelite video feeds are streamed on distributed from companies such as Meta and Nvidia through their respective Platforms Metaverse and Omniverse. Both of these companies currently have several large copyright cases filed against them, including Hermes vs Rothschild and Nike vs Stockx, as well as much unrest about their practices regarding their lack of

176. Meta and Nvidia are also widely known to have a problem with "deepfake" creations on their platforms. The term “deepfake” comes from two separate words – deep learning and fake – which uses artificial intelligence technology to create fake pictures or videos in the image of an original video or image. The creator can utilize special software programs to create the picture or video by face swapping. This has become a problem because it can violate the victim’s privacy rights and public image. Many victims of Deepfake technology cite the content for either being obviously explicit and profane, or that these Deepfake are made in their likeness with often certain traits that are altered to make them out of character or spread false information.

177. **Plaintiff King was targeted by Deepfake technology spam and scams through the use of Defendants AR/XR programs, applications and devices.** Deepfakes can cause various types of torts.[20] Plaintiff King herself was targeted by many, and with obvious non acceptance. There are many articles online about "malicious Deepfakes". Plaintiff King encountered Deepfakes who generally copied her physical image, including her name and various personal details (like job, house appliances, accessories, or key rings, or are these NFTs?), her voice, general topics that she had spoken about, as well as things that were in her surroundings. Those who use these Deepfakes have tracked her GPS location, and seem to have tried to encourage others to do so by giving this information out to unknown users of AR programs, applications and devices on the internet.

178. Defendants use of the AR/XR programs, applications and devices violate the Copyright Act proscription against data control in that they did not prepare to properly regulate or record the use of Ilegally viewed and reproduced copyrighted materials, such as most all copyrighted types of materials listed above that could be viewed or replicated by watching illegal satelite video streams.

179. The Defendants negligant practices concerning their methods lack thereof for compliance to necessary regulation and record keeping of activities on their AR/XR programs, applications and devices caused much harm to the Plaintiffs. Indeed, the harm to Plaintiff King from this conduct is substantial. Plaintiff King suffered substantial injuries and as alleged herein is due damage compensation and injuction from the negligant practices concerning the use of AR/XR programs, platforms, applications and devices.

180. Plaintiff King was victimized bcause of the illegal data use and practices on the AR/XR devices, programs, platforms and applications had no way of reasonably avoiding the injury they suffered.

181. Plantiff King is entitled to:

a. Injunction from future illegal data collection and use practices in violation of the Copyright Act

b. Actual damages abd/or stauatory damages

c. Punative damages; and

d. Reasonable attorneys fees.

COUNT VI
Violations of California's Consumer Privacy Act

182. This cause of action is brought pursuant to California's Consumer Privacy Act.

183. The California Consumer Privacy Act provides the right to know about, delete, correct, opt-out or limit the personal information a business collects about them and how it is used and shared;

184. Defendants have violated California's CPA proscription against data control in that they do not have proper methods for the regulating and recording activities conducted through their programs, applications and devices, including the right of persons who may have had their personal data illegally collected and employed.

185. Defendants do and have not made it available to Plaintiff King or the

members of the class concerning to know about, collect, delete or limit the personal information that the AR/XR programs, application and device businesses and users collect about them and how it is used and shared, including the rampant misuse live, illegal satelite video streams, and of Deepfakes and various other illegal conducts carried out through the use of AR/XR programs applications and devices.

186. The Defendants negligance concerning not having proper regulatory and record practices caused much harm to Plaintiff King. Indeed, the harm to the Plaintiff from this conduct is substantial. Plaintiff King suffered a substantial injuries and is as alleged herein is due damage compensation and injunction from both the Defendants bad practices.

187. Plaintiff King was victimized bcause of the illegal data use on the AR/XR devices, programs, platforms and applications, and had no way of reasonably avoiding the injury they suffered.

188. Plaintiff King is entitled to:

a. Injunction from future illegal data collection and use practices in violation of the California Consumer Privacy Act;

b. Actual damages;

c. Punative damages;

d. Reasonable attorneys fees.

COUNT VII

Violation of Code of Civil Procedure 527.6 and California Penal Code 646.9

189. This act is brought pursuant the Code of Civil Procedure Section 527.6, and California Penal Code 646.9.

190. CCP Section 527.6, Prohibits harassment when (a) (1) A person who has suffered harassment as defined in subdivision (b) may seek a temporary restraining order and an order after hearing prohibiting harassment as provided in this section. Section be goes on to note that the requirement are 1- a course

of conduct that involves repeated conduct that evidences a call ntinuity of purpose; 2- a credible threat of violence being, that being: a knowing and willful statement or course of conduct that would place a reasonable person in fear for the person's safety or the safety of the person's immediate family, and that serves no legitimate purpose. And 3 - "Harassment" is unlawful violence, a credible threat of violence, or a knowing and willful course of conduct directed at a specific person that seriously alarms, annoys, or harasses the person, and that serves no legitimate purpose. The course of conduct must be that which would cause a reasonable person to suffer substantial emotional distress, and must actually cause substantial emotional distress to the petitioner. 6-"Unlawful violence" is any assault or battery, or stalking as prohibited in Section 646.9 of the Penal Code, but does not include lawful acts of self-defense or defense of others.

191. California Penal Code 646.9. requires proof of being repeatedly harassed or followed another person; and that they made a threat placing the person in fear for his or her safety or for the safety of family.

192. Plaintiff King has large amounts of proof of being repeatedly followed and harassed with no legitimate purpose by users of the AR/XR devices, programs, platforms and applications. The actions and threats that were made upon her have both already harmed her safety, and put her in fear of it.

193. As a result of the stalking ad harassment, Plaintiff King suffered various forms of injuries including physical, mental/emotional, and fiscal.

194. Plaintiff King is entitled to:

a. Injunction from future harassment in the form of illegal data collection and use practices in violation of Civil Code Procedure 527.6 and California Penal Code 646.9;

b. Actual damages and/or statutory damages;

c. Punitive damages; and

d. Reasonable attorneys fees.

COUNT VIII
Violation of California Civil Code Section 3344

195. This action is brought pursuant to California Penal Code Section 3344.

196. The California Civil Code Section 3344 **protects the right of publicity of natural living persons. This includes their name, voice, signature, photograph (including photographic reproduction, still or moving; video; and live TV) and likeness.**

197. These kinds of data belonging to the Plaintiffs were indeed illegally view, reproduced and distributed as secondary content through the use of Defendants' AR devices, programs, platforms and applications, and included such things as the the victims name, voice, various personal details, image likeness and more.

198. **Having such sensitive personal information revealed, alongside address, GPS location, and various types of other sensitive data revealed any time, to unknown users of the AR/XR devices, programs, platforms and applications put Plaintiff King at enourmous and foreseeable personal risk, which did injure her. The Plaintiffhas been a victim of copyright infringments and Deepfake technology that is used to incite unauthorized persons to stalk and harass her.**

199. **Defendants negligant conduct in not having ready methods to regulate and record activity through their AR/XR devices, programs, platforms and applications, including to regulate and record the use of illegal satelite video footage, copyright infringments, Deepfakes, and various other illegal conducts, constitutes a violation of the California Civil Code Section 3344.**

200. Plaintiff King is entitled to:

a. Injunction from future illegal data collection and use practices in violation of California Civil Code 3344;

b. Actual damages and/or statutory damages;

c. Punative damages;

d. Reasonable attorneys fees.

COUNT IX

Violation of California Business and Prof. Code Section 17200

201. This act is brought pursuant the California Business and Professions Code Section 17200.

202. Califirnia Business and Professions Code Section 17200 prohibits **any unlawful, unfair or fraudulent business act or practice. It also prohibits unfair, deceptive, untrue or misleading advertising.**

203. **Defendants' acts constitute unfair business practices under Cal. Bus. & Prof. Code in that they do promote and currently use AR/XR devices, programs, platforms and applications without properly regulating and recording unlawful conduct on the programs, the softwares, hardwares and users of products.** Moreover, in Plaintiff Kings case, a large amount of users unknown to her had been divulged to sensitive personal information about her such as her address, name, various sensitive personal details(such as accessories, tax documents or house keys are now NFTs?), and GPS location.

204. Defendants' conduct is immoral and unethical, offends established public policy, and is substantially injurious to Plaintiff King.

205. Defendants' violations continue to this day. Pursuant to California Business and Professions Code § 17203, Plaintiff King seeks damage compensations for various types and degrees of injuries they suffered, and injunction from the Defendants future lack of regulation and record-keeping methods involving the use of AR/XR programs, applications and devices.

206. Plaintiff King is entitled to:

a. Injunction for future illegal data collection and use practices in violation of California Business and Prof. Code 17200;

b. Actual damages and/or statutory damages;

c. Punative damages; and

d. Reasonable attorneys fees.

COUNT X

Violation of The FTC Act, 15 USC 45 prohibiting unfair or deceptive acts or practices in or affecting commerce.

207. This cause of action is brought pursuant to The FTC Act, 15 USC 45.

208. **The FTC Act, 15 USC 45 prohibits "unfair or deceptive acts or practices in or affecting commerce".**

209. **Defendants breached the FTC Act in that they benefitted from the promotion and use of AR/XR programs, applications and devices that they knew may breach the civil, human, privacy and copyright rights of the Plaintiff, by the unauthorised collection and harvest of personal data, and without proper methods to regulate and record any unauthorised or illegal conducts made through those AR/XR devices, programs, platforms and applications. This caused the Plaintiffs to be the target of individuals who use their AR/XR devices, programs, platforms and applications who stalked and targeted her by her GPS location, causing injuries.**

210. The Defendants involvement in the promotion and use of such devices, programs, platforms and applications is material, and has caused significant lawful violations which have caused her several types and degrees of damages.

211. **By law, companies are required to enforce the safe and lawful use of their products. Augmented Reality products, are no exception to the law.**

212. **The Plaintiff was injured in numerous ways by the Defendants use and promotion of AR/XR devices, programs, platforms and applications.**

213. **Defendants lack of effective policies and regulation regarding their AR/XR devices, programs, platforms and applications compliance to applicable laws, have caused widespread, documented infractions that led to the injuries to**

often unsuspecting victims, including Plaintiff King.

214. As a proximate result of the Defendants conduct, Plaintiff King suffered several types of severe damages.

215. Plaintiff King is entitled to :

a. Injunction from future illegal data collection and use practices in violation of the FTC Act 15 USC 45;

b. Actual damages and/or stauatory damages;

c. Punative damages; and

d. Reasonable attorneys fees.

COUNT XI

Violations of Federal Employment: Penal Code 2635.101; Basic Obligation of Public Service; 2365.502- Impartiality in Performing Official Duties; 2635.702- Using Public Office for Personal Gain; 2635.705- Use of Official Time; 2635.802 Conflicting Outside Employment and Activities; 2635.902- Related Statutes (a-ll).

216. These causes of action are brought pursuant the above listed Penal Codes regarding Conduct in Offices.

217. Defendants Google, Decurusviolate Penal Code 2635.502- mandating Impartiality in Performing Official Duties because the use of AR/XR entails violations of current law, and the use is often accompanied with typical scams, thefts and frauds that occur on AR/XR channels and platforms such as those that run on Blockchain technology.

218. Defendants violate Penal Code 2635.702 of Using Public Office for Personal Gain because they use the AR/XR machines and programs in such a manner with live streamed video and audio footage from unwilling participants, that the action is self-centered and almost treat the act skin to an entertainment movie or radio show. They also speak to other employees and members of the public about subjects that they see or hear through this use of AR/XR-- in fact, they use this method of communication, through talking about AR/XR to others, more than they use many other ways if normally communicating and being realistic and of themself. As a matter of fact, Plaintiff King's life is not a radio show, and many of

the employees know that they are pursuing Defendants when they are using it.

219. Defendants violate Penal Code 2635.705 (b) concerning the Use of Official Time because they use and encourage the use of illicit AR/XR devices in unison with their time on duty, which impairs their ability to do perform their duties correctly and impartially.

220. Defendants violate Penal Code 2635.802(a)(b) concerning Conflicting Outside Employment and Activities because (i) they violate statues listed in 2635.902 and (ii) that their ability to perform their official duties are materially impaired by the use of AR/XR devices and programs while they are on official time.

221. Defendants violate Related Statues 2635.902 (a)-(e), I, j, m, l, o, r, s, v, w, x,z, (aa-ll).

222. In relation to statues governing official employees in regarding the use of AR/XR devices, program, platforms and applications, all of the statues may use the following pre-empt as cause for their actions:

- "AR/XR devices can be in nature uncertain and semi-private when used. There is not a known way to use the technology appropriately in social settings, as immersion is an anti-social verb itself. There are means for persons to "imply" things with reference to the audio, textual and visual material that they consume while interacting with real-time or past-time AR/XR content. When they use these things to socialize on the job, their conduct towards other employees, customers, or public policy itself could be rude and maliciously mannered; they could also say and do things that break public policy. As well, they do not have to speak themself. They might just physically loiter in harasive manners, and when they respond to the preset-real-time content, they would blame any bad action or decisions that they made within the context of that content, either on the content itself, or they would often try to reject the reality of its existence in order to get away with those bad actions and decisions." Again, this pre-empt can be used to

apply to the reality and risk of the following stages, as AR/XR devices, programs, platforms and applications that use real-time video and audio footage can and have been used to stealthily violate the following policies of public office:

223. (a) The prohibition against solicitation or receipt of bribes (18 U.S.C. 201(b)

224. (b) The prohibition against solicitation or receipt of illegal gratuities (18 U.S.C. 201(c)).

225. (c) The prohibition against seeking or receiving compensation for certain representational services before the Government (18 U.S.C. 203).

226. (e) The post-employment restrictions applicable to former employees (18 U.S.C. 207, with implementing regulations at parts 2637 and 2641 of this chapter).

227. (i) The prohibition against receiving salary or any contribution to or supplementation of salary as compensation for Government service from a source other than the United States (18 U.S.C. 209).

228. (j) prohibition against solicitation or receipt of gifts from specified prohibited sources (5 U.S.C. 7353).

229. (l) The prohibition against fraudulent access and related activity in connection with computers (18 U.S.C. 1030).

230. (m) The provisions governing receipt and disposition of foreign gifts and decorations (5 U.S.C. 7342).

231. (o) The prohibitions against certain political activities (5 U.S.C. 7321 through 7326 and 18 U.S.C. 602, 603, 606 and 607).

232. (r) The prohibition against employment of a person convicted of participating in or promoting a riot or civil disorder (5 U.S.C. 7313).

233. (s) The prohibition against employment of an individual who habitually uses intoxicating beverages to excess (5 U.S.C. 7352).

234. (v) The prohibition against fraud or false statements in a Government matter (18

235. (w) The prohibition against concealing, mutilating or destroying a public record (18 U.S.C. 2071).

236. (x) The prohibition against counterfeiting or forging transportation requests (18 U.S.C. 508).

237. (z) The prohibitions against disclosure of classified information (18 U.S.C. 798 and 50 U.S.C. 783(a)).

238. (aa) The prohibition against disclosure of proprietary information and certain other information of a confidential nature (18 U.S.C. 1905).

239. (bb) The prohibitions on disclosing and obtaining certain procurement information (41 U.S.C. 423(a) and (b)).

240. (cc) The prohibition against unauthorized use of documents relating to claims from or by the Government (18 U.S.C. 285).

241. (dd) The prohibition against certain personnel practices (5 U.S.C. 2302).

242. (ee) The prohibition against interference with civil service examinations (18 U.S.C. 1917).

243. (ff) The restrictions on use of public funds for lobbying (18 U.S.C. 1913).

244. (gg) The prohibition against participation in the appointment or promotion of relatives (5 U.S.C. 3110).

245. (hh) The prohibition against solicitation or acceptance of anything of value to obtain public office for another (18 U.S.C. 211).

246. (ii) The prohibition against conspiracy to commit an offense against or to defraud the United States (18 U.S.C. 371).

247. (jj) The prohibition against embezzlement or conversion of Government money or property (18 U.S.C. 641).

248. (kk) The prohibition against failing to account for public money (18 U.S.C. 643).

249. (ll) The prohibition against embezzlement of the money or property of another

person that is in the possession of the employee by reason of his employment (18 U.S.C. 654).

250. Plaintiff King has received awful service and experiences with the employees on many occasions. In most of these situations, she is not being serviced properly at all by any means, and is placed instead in situations where she must defend herself from the onslaught of privacy-invading harassment that incurs even when she leaves the space of the employee. This has caused her to be put under large amounts of prolonged stress and in some occasions has put her directly into situations that are dangerous and wrong for her, either based on the employees malicious intent or own unchecked bad judgement. As a direct and proximate result of Defendants use of AR/XR devices, programs, applications and platforms that use real-time satellite video footage, the Plaintiff on numerous occasions suffered many types of damages from the above listed Penal Codes and Related Statues and more.

251. Plaintiff King is entitled to:

a. Injunction from the current and future use of AR/XR devices, programs, platforms and applications that display real-time video, audio, or text footage of Plaintiff King, or any other person, to employees of ANY organization while they are working, including Goverment organizations; as well as injunction of it use it's by any US citizen-- all of which are already illegal.

b. Actual damages and/or stauatory damages;

c. Punative damages; and

d. Reasonable attorneys fees.

COUNT XII
Violation of Criminal Law

252. These causes of action come pursuant the Criminal Laws and Procedures as cited in CALCRIM.

253. All causes of actions have already been met, and the Plaintiff are likely to happen if AR/XR continues to go unregulated.

254. In relation to the following Crminal Codes regarding the use of AR/XR devices, program, platforms and applications that use real-time video and audio footage, all of the Codes may use the following pre-empt as cause for their actions:

- "AR/XR devices can be in nature uncertain and semi-private. There is no known correct way to use AR/XR devices and programs in social settings, as version itself is an anti-social verb. There are means for persons to "imply" things with reference to the audio, textual and visual material that they consume while interacting with real-time or past-time AR/XR content. When they use these things to socialize on the job, their conduct towards other employees, customers, or public policy itself could be rude and maliciously mannered; they could also say and do things that break public policy. As well, they do not have to speak themself. They might just physically loiter in harasive manners, and when they respond to the preset-real-time content, they would blame any bad action or decisions that they made within the context of that content, either on the content itself, or they would often try to reject the reality of its existence in order to get away with those bad actions and decisions." Again, this pre-empt can be used to apply to the reality and risk of the following CALCRIM Criminal Codes, as AR/XR devices, programs, platforms and applications that use real-time video and audio footage, can and have been used to violate upon the Plaintiff:

255. Disturbing the Peace- Penal Code 415, 415.a(1);

256. Loud Noise- Penal Code 415(2), 415.5(a)(2);

257. Loud Noise, Otherwise Offensive Words, Code 415(3), 415.5(a)(3);

258. Evidence of Uncharged Conspiracy- Penal Code 184;

259. Accessory and Solicitation- Penal Code 32;

260. Solicitation- Penal Code 65(e), 664/187, 272;

261. Compelling to Committ Solicitation- Penal Code 31;

262. *Corp Officers- 24 CAL 446, 456-458;

263. Manslaughter- Penal Code 192(a);

264. Mayhem- Penal Code 205;

265. Abuse or Injury to Child, Elder or Dependant Adult- Penal Code 273ab(a);

266. Simple Battery- Penal Code 243;

267. Uncharged Domestic Violence- Penal Code 13700, Family Code 6211- Evidence of Charged Domestic Violence- Evidence Code 355;

268. Assault With Weapon or Force Likely to Injure- Penal Code 240, 245(c)(d);

269. Continuous Abuse- Penal Code 288.5(a)- Continuous Abuse: Annoying a Child in a Dwelling- PenalCode 647 (a-c);

270. Obscene or Harmful Material- Penal Code 288.2(a), (1),(2); Penal Code 311.6;

271. Possession of Incendiary Device- Penalties Code 453;

272. Arson- Great Bodily Innjury- Penal Code 453;

273. Felony/Misdemeanor Committed to Benefit of Criminal SG- Penal Code 186.22(b);

274. Robbery- Penal Code 211;

275. Burglary- Penal Code 459;

276. Theft- Penal Code 487;

277. Theft by an Employee or Agent- Penal Code 487(b)(3);

278. Theft by False Pretense- Penal Code 484;

279. Extortion- Penal Code 518, 519;

280. Assault with Weapon to Cause Injury or to Committ Another Offense- Penal Code 240, 245(1-4), (b); Penal Code 220(a)(b);

281. Simple Assault on Specified Person/Locations- Penal Code 240-241;

282. Brandishing Firearm/Deadly Weapon- Penal Code 417(a)(1)(2);

283. Rape- Penal Code 261 (a)(2)(6)(7);

284. Battery- Penal Code 242, 243.4(e),(l);

285. Sexual Battery- Penal Code 242, 243.4(a), (d)- Sexual Battery on Specified Persons/Locations- 242, 243(b),(c),(2);

286. Rape of Unconscious Woman- Penal Code 261(a),(4), 262(a),(3); Rape of Disabled Person- Penal Code 261(a),(1)- Rape by Fraud, 261(a),(5);

287. Oral Copulation by Force- Penal Code 287 (C)(2)(3)(K)- Oral Copulation In Concert- 287(d); Oral Copulation By Fraud- Penal Code 287(a)(l); Oral Copulation While in Custody- 287(a)(e);

288. Lewd and Lascivioys Action- Penal Code 288(a)(b)(1);

289. Involving Prisoners:

290. Assault and Battery- Penal Code 4500;

291. Assault by Prisoner- Penal Code 4501;

292. Inciting Riot in a Prison/Jail- Penal Code 404.6(c); Possession of Contraband- Penal Code 4502;

293. Firearm/DW/Explosive in Jail- Penal Code 4574(a)- Bringing to Institution-Penal Code 4574(a-c);

294. Misappropriation of Public Money- Penal Code 424(a)(1-7);

295. -was resp for receiving/safekeeping or transferring/distributing public money while: took money for __ w)o legal authority, made profit from or used, made false action/entry, changed/ hid account of money, willfully____

296. Vandalism- Penal Code 5;

297. Loitering- Penal Code 647(h)- Peeking- Penal Code 647(I);

298. Tresspass- Penal Code 601(a);

299. Right to Defend Real or Personal Propert- Civil Code 50: - Right to Self Defense, Right to Ehect Tresspasser, when resident is reasonably afraid of injury- Penal Code 198.5;

300. Possession of Material to make DD- Penal Code 18720;

301. Sale/Transport of DD- Penal Code 18730;

302. Offer to sell/Distribute DD- Penal Code 18730;

303. Manufacturing a Controlled Substance and Offering- Health and Safety Code 11379.6(a), 11362.3- Receiving Money From- Health and Safety Code 11370.6;

304. False Personation- Penal Code 529(a);

305. Fraud Sale/Transfer/Conveyance of PII- 530.5(d), (l);

306. Identity Theft, Unauthorized Use of PII- 530.5(a);

307. Fraudulent Possession of PII- Information Code 530.5(a), (1-3);

308. Forgery- False Signature- Penal Code 470(a); Check Fraud- Penal Code 476; Filing False Documents-Penal Code 115; Making Counterfeit Access Cards/Accounts- Penal Code 484(f)(a); False Signature- Penal Code 484 (f)(b)

309. Plaintiff King has suffered injuries of the violations of each of these codes begining in 2019. There are documents and other proofs asserting these facts.

310. When the FCC repealed the Net Neutrality rules, they also launched AR/XR program initiatives for Goverment agencies in it's place. Those programs employ AR/XR devices, platforms and applications to view illegally-taken real-time video and audio footage of Plaintiff King herself. Plaintiff King believes that the FCC made this choice illigitimately, as they knew it would make her a target of stalking, harassment, and various other types of crime. The FCC fully knew that, but still intended to illegally display footage of the Plaintiff to unregistered, unrecorded, unauthorised users of the AR/XR products. This led directly to the Plaintiff becoming injured on many occasions, and she is still very unsafe.

311. Plaintiff King is entitled to:

a. Injunction from the current and future use of AR/XR devices, programs, platforms and applications that display real-time video, audio, or text footage of Plaintiff King, or any other person, to employees of ANY organization while

they are working, including Government organizations as well as injunction of it use it's by any US citizen-- all of which are already illegal.

b. Actual damages and/or stauatory damages;

c. Punative damages; and

d. Reasonable attorneys fees.

COUNT XIII
Violation of Federal Tort Claims Act

312. This cause of action is brought pursuant the Federal Tort Claims Act 28 USC 1346.

313. All forgoing paragraphs are re-alleged herein. Based on the Conduct by Goverment employees who use AR/XR devices, programs, platforms and applications to stalk and harass the Plaintiff, who had suffered many violations under the Codes of Federal Regulation and CALCRIM Penal Codes, the Plaintiff declares the employees in viation of the FTCA's proscription agsinst wromgful or negliant actions by Gocerment employees causing injuries.

314. The Plaintiff's injuries and damages have been extreme and constant, and are still ongoing, despite the exhaustion of administrative remedies. She has suffered many injuries from the use of the devices and programs, all of which had been listed above. She demands an end to the senseless, immoral and extremely injurous conduct by the employees.

315. Plaintiff King is entitled to:

a. Injunction from further violation of the FTCA act by regulating the use of AR/XR devices, programs, platforms and applications use by Goverment employees;

b. Actual damages and/or statustory damages;

c. Punitive damages, and;

d. Reasonable attorneys fees.

COUNT XIV
Unjust Enrichment

316. This cause of action is brought pursuant to the Unjust Enrichment Clause, which states: The defendant received a benefit at the plaintiff's expense; and under circumstances that would make it unjust for the defendant to retain the benefit without commensurate compensation.

317. Defendants, in promoting and using AR/XR devices, programs, platforms and applications in the State of California, have engaged in a consumer-oriented business practice or act.

318. Defendants knowingly promoted used their products knowing that they used illegal types of satellite and drone video footage, and that there were no methods established to regulate or record the proximate illegal use of those products as required by law.

319. **In addition, the AR/XR program that the Defendants use, revolves specifically around Plaintiff King, in that illegal aerial video footage is streamed and recorded to the AR/XR devices and platforms, which are transfered to AR/XR Headsets, glasses, and contact lens to run an AR/XR-centric "program". This program, as described in all earlier paragraphs, distributes information to unknown, unauthorized users of the hardware and software, which they use to stalk, cyberstalk and harass individuals by GPS location, often dressing and saying words as to copy the person, or simply harass, or create deepfake technology to stalk and harass that person online. They might also threaten to assault you or steal your possessions, which has happened to Plaintiff King several times due to the Defendants conduct.**

320. Defendants FCC, Meta, Nvidia, Maxar Technologies, Google, Securus Technologies, Global Tel-Link, Inter Active Corp, Match Group all use these programs themselves, and encourage the use and acceptance of it to customers, many of which customers have horribly harassed Plaintiff King in various extremely unacceptable ways, and even have stolen from and threatened to

321. The employees often take on the name and visual and vocal appearance of both herself and other specific individuals from past occurances. The drama created by stalking and harassing her has seemed to serve as a distraction, in that workers do not have to do their jobs properly-- no one is looking at THEM-- not for long at least. So, the workers using these technologies are not paying very much attention to doing their jobs properly.

322. In addition to not doing their jobs properly, they seem to use both visual and audio from the streaming footage of the Plaintiff to take around with them on their electronic devices throughout the day. Given that this is **Plaintiff King's** time, voice, image and life on her own properties, and that the employees use it while they are working and in relation to their customers, Plaintiff King is obviously suing them for unjust enrichment, and demands repayment and injuction from the pathetic practice.

323. As a direct and proximate result of the Defendant's conduct, the Defendants have been unjustly enriched through the use and promotion of their AR/XR devices, programs, platforms and applications. Plaintiff King was injured, in several forms and on many occasions, by the Defendants and by users of the Defendants AR/XR programs, devices, platforms and applications, and yet the Defendants had been sitting in offices earning money for themselves over it.

324. Defendants' violations continue to this day. Pursuant to the Unjust Enrichment clause, Plaintiff King seeks such orders and judgments that may be necessary to disgorge Defendants' ill-gotten gains and to restore to Plaintiff King any money made from the companies illegal data practices on their AR/XR devices, programs, platforms, and applications a result of Defendants' wrongful conduct.

325. Under the circumstances, it would be against equity and good conscious to permit Defendants to retain the ill-gotten benefits that they received through the

Plaintiff, in light of the fact of their obvious knowledge and the perceived consequences of their actions to Plaintiff King's safety and civil rights. As well, though they had known of their actions likely consequences, their devices, programs, platforms, and applications lacked regulation methods enough as to constitute gross negligance.

326. Defendants' conduct is immoral and unethical, offends established public policy, and is substantially injurious to Plaintiff King.

327. Plaintiff King is entitled to:

a. Injunction from future illegal data collection and use practices in violation of unjust enrichment statues;

b. Actual damages and/or stauatory damages;

c. Punative damages; and

d. Reasonable attorneys fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff King demands judgment on behalf of themself, providing such relief as follows:

A. An order of injuction from the current, unregulated practices concerning the use of their AR/XR devices, programs, platforms and applicatons, and fNIRS technologies, namely that they may not view, receive or send illegal satelite or drone video, audio or fNIRS footage, particularly and especiallt of the Plaintiff.

B. An order requiring that the company Maxar Technologies, as well as all similar satellite companies, is confronted about their mis-use of satellite technology, pays ramifications to the Plaintiff, and be regulated with Spectrum Monitoring technologies in order to detect and prevent future mis-use.

C. An order requiring that the use of fNIRS technology be put to a stop, that is both for remote eye vision tracking and brain-computer interfaces (BCI).

D. An order for the neurodata and eye vision data that BCI technologies and fNIRS satellite video scanners (Near-Functional Infrared Spectroscopy scanners) collect, even and especially through satellite video fNIRS scans, be classified as biometric data so that their use can be regulated by federal and state data privacy laws.

E. An order for more strict biometric data privacy laws and better methods to carry them out.

F. An order to hold Defendants liable for correcting their practices concerning the lack of regulation and record-keeping on the AR/XR devices, programs, platforms and applications that they use for commercial purposes in their facilities systems. Such that the Defendants will account for, and implement a constructive system for logging and monitoring activity conducted through their AR/XR devices, programs, platforms and applications so that they

can apply proper algorthms to automatically remove, ban, and record unlawful activities by users and unlawful content in the case that they may be held accountable for breaking rules, or laws;

G. An order requiring the County, State and Federal Goverment to evaluate AR/XR Technologies: their illegality, dangers, and lack of appropriate use within both federal agencies and the community at large.

H. An order requiring the County, State and Federal Government to offically classify and regulate AR/XR devices, programs, platforms and applications in the Industrial Product Market, and to read the Plaintiff's attached documents which include: Referencial Material Regardng AR/XR Use in Goverment(4 pages), Responses to Referencial Maierial(2 pages). AR/XR Industrial Classification(5 pages), and AR/XR Device Evaluation under ISO-2100 Standards(4 pages). These attachments come down to the Evaluation under ISP-2100 Standards, in which the Plaintiff shows that AR/XR devices, programs, platforms and applications are high risk and dangerous enough to be likened to explosives and firearms.

I. An order for the illegalization of cryptocurrency, including all Blockchain and NFT activities, especially Ethereum and Ethereum platforms such as Minds.com. Meta's Metaverse, for one, may not use Cryptocurrency, or Blockchain-based NFTs in its games. Especially, they may not use Blockchain or NFTs that replicate anything to do with the Plaintiff herself, or any of the other Related Induviduals, topics or events within the AR/XR timespan of the old military base project, as relates to her filed case in Lake County CA.

J. An order for the current use of AR/XR devices, programs, platforms, applications and fNIRS technology within the County to be regulated and put to a stop. This includes the use by government agencies, businesses, and all other residents of the county. The Plaintiff has been routinely interrogated about things such as housing and resources by residents of the county,

and yet she is not authorized to know or speak of such issues. She suggests that, as a government which tries to impose security standards, that laying off the use of satellite video surveillance, fNIRS and AR/XR products, in favor of adopting simple Policies enforced with Encryption and Grounded Theory, security will be much higher and more solid in figures.

K. An order requiring the Drone market to be more strictly regulated, requiring drones and drone makers to follow policies on the licensing, use and software/hardware regulations of drones. It might require that companies who create drones also give out tracking information to government archives when the drones are created and sold.

L. An order requiring the County, State and Federal Governments to create 2 new agencies, one dedicated to Spectrum Monitoring in order to regulate satellites, and the other to Drone Regulation. Spectrum Monitors is us a must, and as well Drone Regulation for state and local governments is a must. This might involve creating a trust fund for Spectrum Monitors and Drone detection, Drone classification and identification, and Drone location and tracking devices that might be requested by local governments on demand to combat the use of rogue satellite and drone violations.

M. An order for a County, State and Federal-wide declaration statement and due processes on the War on Crime and Drugs. This includes creating and deploying tactics and methods to reduce violations by general populaces, and holding known terrorists accountable. Each time a convicted felon or an organization or entity accused of previously violating the law re-violates their probation or other legal orders, they should suffer a new electronically-administered fine to pay. This helps to both deter those actions, and fund the government.

N. An order to appeal for the resurrection of Death Penalty prosecutions for repeated, intentional, violent and extreme crime.

O. An order for Law Enforcement to begin searching for, compensating and destroying AR/XR products such as Glasses, Headsets, and the very popular Contact Lens amoung their inmate population. These devices are not permitted to any inmates or arrested persons. Such continuance would be jail break, which is very illegal. This will extend to law enforcement officers as well: they are not permitted to use any of these devices or technologies on duty. Grounded Theory and Homomorphic Encryption should be put into place as soon as possible.

P. An order for any federal grants for crime control and prevention especially to Telecom companies, such as amendamants to the Violent Crime Prevention and Law Enforcement Act or any other outlet, to remain within the public sector and not the private sector. Too much abuse happens when these grants are given to the private sector. Such provisions should only be for trustable federal agencies and operations to design appropriate encryption and application standards. This is the Crux of the Plaintiff's complaint about Telecom companies.

Q. An order for County Offices to prosecute the local Jack in the Box corporation for illegally stalking, harassing, and attacking the Plaintiff, as well as their gross negligence of working violations, AR/XR use, and all of the actions and motives listed in the Plaintiff's filed federal case in San Francisco District Court of Northern California against Jack in the Box corporation and employees. These persons and entities are guilty of fraud, stalking, harassment, extortion, working violations, drug and alcohol abuse and drug trafficking. They should be prosecuted, regulated, and the money assumed from their behaviors seized and reclaimed, as well as the loss of their business liscences. Several of the Related Induviduals in the Plaintiff L's case are affiliated with the local Jack in the Box. These include Nicole and Rene Perez, Momica Flores, Vicente Colacion, Daniel Schmitt, and the Motorcar and cycle hobbyists. This business should be prosecuted for crimes against both the Plaintiff, and the County and State Governments.

R. An order for a County and state-wide mandate to search for, compensate and destroy AR/XR

devices on any person with whom there is evidence that are employeed for wages anywhere or has violated any laws, or the Plaintiff's sets of orders. Contact with the sellers and manufacturers of these devices might also be noted for future regulations and charges.

S. An order for any police calls or reports to all Law Enforcement agencies that ask responses to a caller's lack of money, housing or jobs, or other non-emergency related requests to be categorized as instantly invalid, and be thrown away and the phone numbers blocked.

T. An order for Jail and Prison to be officially, publicly and loudly categorized as a place for punishment for violationing the law. Jails and prisons are for punishment, and not for resources.

U. An order for a correct amount of homeless shelters, tiny house areas to be erected. These should be limited and very rule-based. These are different from persons with lawful disabilities that have gone through due process. They are low-budget, low-maintanance and temporary. Persons should be absolutely restricted from using AR/XR products while staying there. Homeless shelter/other shelter staff should be mandated to follow the same policies in regards to the restriction of AR/XR devices, in that they are actively searched for, compensated and destroyed upon discovery. This can take the pressure off of jails to house persons, because jails are for punishment.

V. An order for Telecom companies, as well as ISPS and internet platform operators, to be more strictly regulated. These entities may not make products that are for common-use public consumption that incorporate live, constant and real-time human operation in the background. Technology is developed to the point that human-opetated services for phone data, internet data and website use are both unnecessary and unconstitutional. Telecoms, ISPs and website platform owners should, when regarding general traffick on their platforms and services, only use homomorphic encryption to filter, record and regulate user activity, when these Telecoms,

ISPs and website platform owners operate any platforms or services that are meant for large user bases– that is, people from different backgrounds, religions, ethnicities, ages and priorities. Their encryption standards should be determined and administered by an official government entity that will construct a Homomorphic Encryption Program to ensure compliance with best practices regarding electronic communications that violate or might violate the law, and design several templates for each for each form of websites to ensure functionality.

W. An order for Google and Meta to become more strictly regulated. They must comply with regulations proposed to be enforced on other Telecom, ISP and internet websites, meaning it will be filtered with encryption and the applications will be run by AI-- NOT humans. They must cease their behavior regarding android applications within the Google Play Store that incorporate theft of personally identifiable information from any citizens. The includes electronically generated images or statements that reference or mimic induviduals, as well as human-generated lookalikes of "famous" persons related to the AR/XR program in California and Washington. They cannot feature these things in places such as the Google Play Store applications or advertisements on those applications. If Google and Meta are to operate in the public sector, must not make any of it's content geared towards any specific persons or entities.

X. An order for Meta, and similar internet and technology companies, to be forced to follow anti-harassment and biometric privacy laws. On Facebook, they can no longer fill a users page with advertisements-- the number of advertisements or "suggested posts" as they call these-- posts on a Facebook feed that a user is not connected with-- must be limited, and customizable as to what a particular user wants to see. As well, they should not advertise their "people you may know" section on the front page-- a user can individually select that feature through a link. A

user should mostly only see content that they added themself. Their use of AR/XR must be stopped and the content they advertise must be minimalistic and neautral for the most part. They should comply with CCPA.

Y. An order declaring Defendants' conduct to be in violeton of applicable law;

Z. An order requiring that the FCC and FTC begin to properly regulate all companies, especially telecom and internet companies, using Homomorphic Encryption and Grounded Theory standards, and the Plaintiff's suggested Homomombhic Encryption methods such as those in the attached documents of Privacy Protective Surveillance, as well as references to Two Hat Web Filtering, which is capable of providing automated regulation for ISPs and Telecoms, to filter, record and regulate illegal and risky content on their websites and platforms without invading the privacy and various other rights of citizens of users.

AA. An order requiring an accounting for, and imposaion of, a constructive trust upon all monies received by Defendants as a result of the unfair, misleading, fraudulent, and unlawful conduct alleged herein;

AB. An order awarding injunction, disgorgement, punitive damages, and/or monetary damages in an amount to be determined at trial together with costs and disbursements, including reasonable attorneys' fees and costs as allowed by law.

AC. Prejudgment interest at the maximum rate allowable by law.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable. Plaintiffs designate _____ as the place for trial.

Signed,

Jessica King

General Delivery

Lakeport, CA 95453

559-818-7900

jessck12875@gmail.com

Important: Additional Factual Allegations– Added After First Print

XXI. Plaintiff King's experiences with Jack in the Box and their actions that they did do upon her through the use of AR/XR and fNIRS products both constitute abuse and unfair working conditions and a violation of the respect of her person that has continued effect upon her life and employment to this day.

1. According to a work attorney's website, "A hostile work environment exists when the harassment is so severe and pervasive that it alters your ability to do your job. The behavior must be more than just offensive; it must be objectively abusive.The harasser can be anyone in the workplace, including a supervisor, coworker, or even a customer or client. The victim does not have to be the person harassed but can be anyone affected by the offensive conduct. To assess whether behavior is severe or pervasive enough to create a hostile work environment, courts will look at factors such as:[151]

    - How often did the discriminatory conduct occur?
    - Was the conduct directed at you because of your protected status?
    - What type of conduct was it?
    - Would a reasonable person find the work environment hostile based on this"

2. **Plaintiff King criticizes the surveillance techniques of using AR/XR technology to be inefficient for business success, including that of law enforcement, and the moral work-life balance that employees are due:**

    - **One article shows a series of studies aimed at determining if employees who are told that they are being surveilled behaved better or worse, and found that they did behave worse:** "Of course, this survey only determined correlation — so to prove causation, we ran a second, experimental study. We asked another 200 U.S.-based employees to complete a series of tasks, and told half of them that they would be working under electronic surveillance. We then gave them an opportunity to cheat, and found that those who were told they were being monitored were actually more likely to cheat than those who didn't think they were being monitored. Specifically, when we surveyed the participants in our studies, we found that those who were monitored were more likely to report that the authority figure overseeing their surveillance was responsible for their behavior, while the employees who weren't monitored were more likely to take responsibility for their actions. This reduction in agency in turn made the monitored employees more likely to act contrary to their own moral standards, ultimately leading them to engage in behavior that they would otherwise consider immoral."[152]

    - <u>More work on days off and longer hours of work were reported after the Covid-19 Pandemic.</u> <u>SOURCE 1:</u> May 2022: "While the concept of overwork is not new, it reached a pivotal point during the recent COVID-19 pandemic. During this time, the move to work from home and required lockdowns led many people to begin working longer hours due to dissolving boundaries between work and home time. A survey conducted by staffing firm Robert Half in 2020 found that 55% of respondents who transitioned to work-from-home arrangements worked on the weekends, while 34% said they were working more than 8 hours per day on a regular basis.[153] <u>SOURCE 2:</u> Feb 2022: Remote workers are especially vulnerable to exhaustion from 'always on' work, pandemic fatigue, and burnout. Mounting evidence highlights how overwork-related fatigue puts workers at risk.

Employees are 61 percent more likely to incur an injury when working overtime. Working 55 hours or more per week is associated with an estimated 35% higher risk of a stroke and a 17% higher risk of dying from ischemic heart disease. And workers who sit for prolonged periods are at elevated risk of early death from any cause. What's the business impact? Businesses too often take the gamble of hefty OSHA fines to overwork employees. And it's to nobody's benefit. A Stanford study found that productivity declines sharply after 50 hours a week, and after 55 hours, productivity drops so much that putting in any more hours would be pointless. At the same time, overwork-related fatigue is responsible for poor performance on the job, work-related accidents, and mental and physical illness. When people burn out, they disengage from tips ect[154]

- No work-life balance: SOURCE 1: When work starts to take over your life, things start to fall apart. 76% of workers say that their workplace stress impacts their personal relationships, and 66% say that their stress caused sleep deprivation. Suddenly, there is little time to spend with family, take care of yourself, or do the things you enjoy. There's less time to spend with friends or be a part of groups outside of work. When work rules your life, it becomes your identity and your purpose. But there is so much more to life than work. We need balance so we can take care of our mental health and wellbeing.[155] SOURCE 2: The majority of the interviewees described their jobs as highly demanding, exhausting, and chaotic, and they seemed to take for granted that working long hours was necessary for their professional success. However, about 30% of the men and 50% of women in our sample appeared to consciously resist working long hours, describing a variety of strategies they developed for maintaining a healthier work-life balance. While the details of every individual case differed, our study suggested a common mental process that consistently helped this group of professionals to change the way they worked — and lived — for the better. Pat attention to emotions, re-priiotitise . Reprioritize. Increasing your cognitive and emotional awareness gives you the tools you need to put things into perspective and determine how your priorities need to be adjusted. Ask yourself: What am I willing to sacrifice, and for how long? If I have been prioritizing work over family, for example, why do I feel that it is important to prioritize my life in this way? Is it really necessary? Is it really inevitable? What regrets do I already have, and what will I regret if I continue along my current path? Our priorities often shift faster than our day-to-day time allocation habits. The interviewees that described a more positive work-life balance intentionally reprioritized how they spent their time in a way that lined up with their true priorities. One participant described how he still saw himself as a professional, but redefined that professional role to be more inclusive of other valued roles, such as that of parent.[156] SOURCE 3: If your employees are unable to maintain their work-life balance, then it's probably down to them putting in overtime hours. If your employees fail to take time off for "unplugged vacation time" and family events, it strains their personal life and also leads to work-family conflicts. They may also constantly feel like there is "less time" to complete their tasks across a work week – leading them to put in more hours over the weekend to cope. The result? A vicious cycle of overworking continues – constantly diminishing their work life balance. How to spot this? Ensure that you track the breaks, vacation time, and paid time offs (PTOs) that your employees take. If they're seldom utilizing any of the above, it indicates overworking. 5. An inability to relax. If your staff find it hard to relax and unplug due to stress and overexhaustion, then they could be overworking. Overworked employees tend to obsess about their work-related commitments and challenges, making it difficult to relax at their own time. This in turn, leaves no room for their personal life commitments and self-care. Additionally factors like the Coronavirus pandemic (COVID-19) can lead to increased anxiety – making them more reactive to overtime work stress during the next workday. How to spot this?